International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Federated Learning Analysis in Decentralized Systems

Billa Prahas Reddy

Submitted: 01/06/2025 **Revised:** 05/07/2025 **Accepted:** 15/07/2025

Abstract: The growing necessity to protect sensitive health information has led to the rise of federated learning (FL), a distributed architecture for machine learning. Improving the healthcare system becomes necessary during a pandemic. The healthcare industry is continuously making use of numerous AI technology advancements. Because of its decentralized and collaborative approach to constructing AI models, Federated Learning (FL) has gained notice as one such innovation. One of FL's most notable features is that it keeps raw data hidden from prying eyes by keeping it with data sources all the way through training. Because it handles sensitive personal information, FL is more suited to and inevitable in the healthcare industry. Even if there are various privacy and security issues, federated learning (FL) enables multiple institutions to build AI models without sharing data. To be more specific, FL insights can compromise institutional data security. Also, problems can arise with FL when there isn't enough trust between the entities doing the computation. There is an urgent need to clarify the hazards associated with FL because of its increasing use in healthcare. Thus, in this paper, we highlight the literature on privacy-preserving FL as it pertains to healthcare. The risks are highlighted, and methods to lessen them are examined. Researchers in the healthcare industry in Florida can use this review as a resource for information about patient privacy and security in the Sunshine State.

Keywords: *federated learning (FL), AI models, healthcare.*

1. INTRODUCTION

In federated learning, models are trained across numerous clients, such as smartphones or Internet of Things devices, without transmitting local data to a central server. This decentralized method to machine learning is known as "federation" [1]. On the contrary, local models are trained locally on-device, and the only data communicated with a central server are model updates, such as gradients or weights. This data is then aggregated to create a global model.

1.1 Key Benefits

Privacy-Preserving: Lessening privacy concerns, data stays on the local device.

Reduced Latency: For real-time applications, on-device processing can decrease latency.

Scalability: Massive datasets can be trained using distributed methods across multiple machines.

Undergraduate
Computer Science and Engineering
Chaitanya Bharathi institute of Technology
Gandipet, Hyderabad, Telangana
prahasreddybilla@gmail.com

Efficiency: Lessens the burden on data transfer infrastructure, which in turn conserves storage and bandwidth.

Training machine learning models in tandem across nations and companies is at an all-time high due to the proliferation of big data, the lightning-fast progress of machine learning, and the ever-increasing connectivity throughout the world [2]. Data privacy concerns are the main obstacle to healthcare collaboration training since they restrict the sharing of data and the practical application of technically feasible solutions [3]. Therefore, methods that protect users' privacy, like generative adversarial networks, blockchain technology, and federated learning (FL), are receiving a lot of attention. FL, Google's distributed machine learning framework, preserves data privacy while enabling multi-party collaboration; it was announced in 2016. With its emphasis on patient confidentiality, it offers a promising alternative to conventional centralized training in the medical industry [4]. Evidence suggests that FL can handle a wide variety of data types with ease. These include imaging images (e.g., X-rays of the chest for COVID-19 clinical outcome prediction), grayscale images (e.g., skin photos for skin lesion diagnostics and retinal fundus photographs), and histology slides (e.g., for cancer diagnosis, genomics, and the Internet of Medical

Things) [5]. An initial set of participating sites would have their weights for the global model parameters broadcast from a central server in the original FL framework. After that, each site uses its own data to train a local model, which shares its architecture with the global model. It then updates its parameters and sends them to the central server. By keeping all data on-site at all times, this setup avoids the drawbacks of traditional centralized learning, which involves sending raw data to a central location (Figure 1). The server then aggregates the updates from all the sites to update the global model weight [6]. Following this, a fresh batch of participating sites receives the updated global model, which they use to conduct local training once again. We keep doing this until our global model converges. Using FL's larger training datasets acquired from many sources, FL is able to generate a higher-quality model than what could have been produced with the data of a single device or system, all while keeping data privacy at high levels. The approach significantly reduces the expenses associated with collecting data. Furthermore, it has proven to be resilient even when faced with customers having data that is not independent and identically distributed (IID) or has an unequal quantity of data.6 Because of this, FL is a desirable machine learning subject in the healthcare domain, and it is particularly useful in specialized study areas with limited or restricted public data [7].

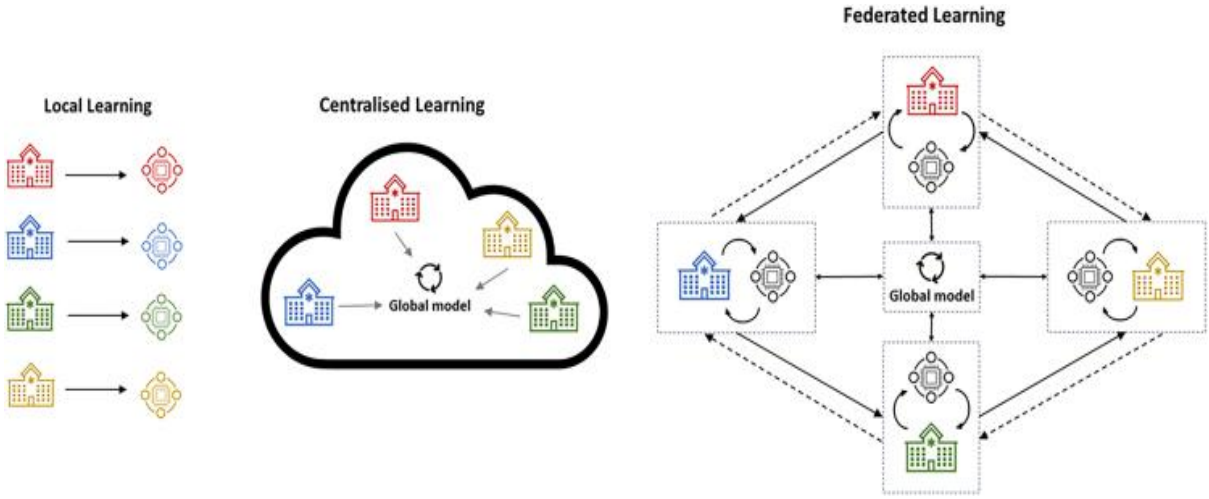

Figure 1. Federated learning as contrasted with centralized and localized learning

Efforts to boost clinical translation are ongoing, but FL has not yet achieved widespread clinical use despite its advantages [8]. In addition to FL's youth as a privacy-preserving technology, studies are continuing to compare it to established machine learning frameworks and evaluate its resilience across a variety of clinical areas. Furthermore, even if FL offers better privacy protection, sharing model updates could still jeopardize privacy. Because of this, more recent FL models incorporate additional privacy techniques such differential privacy and cryptographic methods like secure multi-party computation, blockchain, and homomorphic encryption.

1.2 The rise of Federated Learning

The COVID-19 pandemic has only added to the tremendous expansion of Big Data in the past few years. Since this data is so massive, there has been a surge in interest in artificial intelligence (AI) techniques like machine learning (ML) and deep learning (DL), which teach computers to sift through it all and find insights. The standard procedure for constructing ML/DL models involves transmitting all data generated by all entities to the server or service provider's location, which is typically in the cloud. Only on the server will the whole model-building and training procedure occur. Some difficulties arise with this approach. There are a lot of different, geographically dispersed places to find the data that is required to construct an ML model. Factors like insufficient network connectivity make it difficult to integrate this fragmented data from distant remote places. In addition, a large portion of the data pertains to personally identifiable information. Ensuring the secure transmission of private data across international borders while respecting users' privacy rights is thus a challenging task. It will be more expensive and strain the network's capacity to send massive amounts of data from all across the globe to one central site [9].

Alternatively, an ML model's accuracy improves as the amount of data supplied into it increases. As a result, Federated Learning has emerged as a viable alternative approach to data migration and integration that prioritizes the protection of sensitive information. Clients, which can be smart devices or organizations, and servers, which coordinate the process, work together to train and construct the model in federated learning, a form of distributed ML [10]. Instead of exchanging or transmitting raw data to a server, FL uses it locally on each client. Every client that wants to be a part of it trains an ML model on their own data for a set amount of rounds till some qualifying criterion is satisfied. They change the ML model parameters between iterations and send them to the server to be aggregated. The server sends the aggregated model parameters back to all clients, so they can use them in the next iteration. Until the model converges or the target accuracy is reached, this iterative process is repeated.

2. LITERATURE REVIEW

Data parallelism established a paradigm shift in traditional FL toward centralized aggregation and decentralized learning. The term "data parallelism" describes a scenario in which clients' raw data is created in parallel on-premises and is neither transmitted nor made public. In order to get a global model, all the clients combine their local data to train a model, and then they send the model's parameters to the server. This way, the learning results from all the clients are effectively integrated. The taxonomy of FL frameworks, which includes cross-silo and cross-device FL frameworks, is based on the quantity and type of clients that are part of the learning network [11]. Companies, universities, data centers, etc., that fall within the "clients" category in cross-silo FL often have better communication, greater computing power, and more data to work with. Big mobile or IoT devices are the clients in cross-device FL, and they could run into problems with computation and communication. Regarding variations in client data distribution, another FL taxonomy is taken into account, which includes transfer, horizontal, and vertical [12]. There are fewer users with identical sample features and more clients with similar sample features in horizontal FL. There are fewer shared sample characteristics and more similar users across vertical FL clients. Neither the sample features nor the users of federated TL clients are really similar.

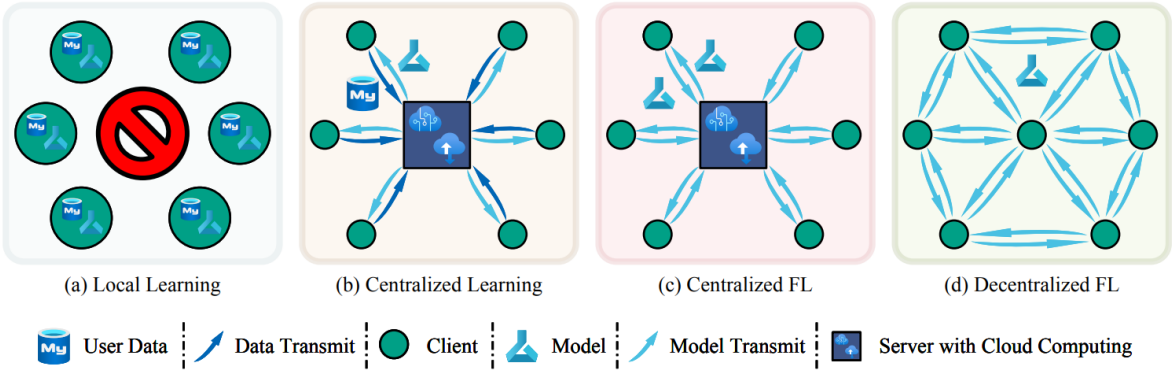

Fig. 2. A demonstration of CFL, DFL, centralized learning, and local learning. (a) Train your clients using data from your local users exclusively. Clients do not converse or exchange raw data with one another. (b) The user data packets are sent to the server by the clients, and then the server uses all the data to train a generic model. After then, every client gets access to the standardized model. c) A client will communicate with the server and transmit the parameters of the model that have been trained locally. After collecting all the local models, the server sends the aggregated global model parameters to every client. (d) Users can collaborate with other users by sharing their locally trained model. Later on, clients build upon this foundation by learning and customizing the model locally, sharing and propagating model parameters with local knowledge, and so on.

Learning at the local, centralized, CFL, and DFL levels is depicted in Fig. 2. Overfitting might occur in the local learning method since each client keeps their own data and trained model and doesn't share it with any other clients or servers (Fig. 2(a)). In contrast, as seen in Fig. 2(b), a centralized learning technique uses raw data transmission in client-server connection to centralize and consolidate learning, but it does not ensure user privacy. Researchers typically compare FL to both of these methods as a

starting point. Centralized client-server architectures (CFLs) rely on a central server to manage, coordinate, and interact with all clients. A client-server conversation is depicted in Fig. 2(c). After learning on local data, clients send the server the parameters of the model that they have trained. In order to create a global model, the server compiles all of the local models and makes it available to the clients. Without server cooperation, clients communicate directly with each other, as seen in Fig. 2(d). The communication network between clients is more heterogeneous due to the lack of consistent server coordination and configuration. With increased confidence in varied versions, DFL dismissing the server can further save communication and processing costs because it is regarded more adaptable.
One explanation is the absence of standardized electronic health records. Because of financial constraints, hospitals in economically disadvantaged areas may not be able to participate in research that need electronic patient data management, which could lead to the continuation of the problems with equity and bias that have already been highlighted. Nowadays, medical imaging practices almost exclusively use electronic data management systems: Almost everywhere in the world, people are using electronic file storage and the imaging data format is called Digital Imaging and Communications in Medicine (DICOM). The CBIS-DDSM dataset, which includes digitized film breast radiographs, is one example of how archival film radiography enables post hoc digitization even in settings where non-digital formats are still in use [13]. The aforementioned achievements of medical imaging AI are driven by digital imaging data that is easily shareable, permanently stored, and remotely available on the cloud. The stringent regulation and protection requirements for patient data are the second major obstacle to conducting AI trials across several institutions and countries. Concerns about data handling, ownership, and AI governance have been sparked by the stringent regulations imposed by both HIPAA and the General Data Protection Regulation (GDPR)25 in the European Union. These regulations demand authentication, authorization, accountability, and, with GDPR, the interpretability of artificial intelligence (AI). Respect for privacy, defined here as the capacity to maintain complete control and confidentiality over one's personal information, is also mandated by scientific, ethical, and moral principles (soft law). In this article, "privacy" refers to the goal of preventing data leaks, whether accidental and intentional (i.e., it is synonymous with "confidentiality").

The novel distributed interactive AI idea of Federated Learning holds great promise for smart healthcare. It enables multiple clients, like hospitals, to engage in AI training while ensuring the privacy of their data. Authors dug deep into FL's potential use in smart healthcare to find out why [15]. First, we will go over the most recent FL developments, followed by the rationale and necessary conditions for implementing FL in smart healthcare. Medical data recording, biomedical image processing, remote patient monitoring, and COVID-19 detection are just a few of the emerging FL applications in healthcare that the authors have provided a comprehensive overview of. Recent studies have suggested FL for use in many Internet of Things (IoT) initiatives, such as intelligent transportation systems and electronic healthcare. One example is how FL has facilitated the expansion of e-health services by enabling ML modeling in the lack of health data [16]. Hospitals and other health data owners can use FL to prevent the exchange of sensitive patient information. Alternatively, medical staff can train the model locally before sending the parameters to an accumulator to use in data collection. Federated learning has shown promise as a way to build revolutionary healthcare systems that are both cost-effective and private [17]. Due to FL, AI models may be trained even in the absence of local data by averaging local updates from several healthcare institutions and smart devices, like IoMT.

However, due to the rapid growth of AI technology, AI has found applications in numerous fields, such as robotics, machine vision, natural language processing, and the Internet of Things (IoT). To be more precise, scientists have sought to improve healthcare sector efficacy by increasing scientific analysis and remedy analysis through the application of AI [18]. For decades, people have speculated about the potential benefits of AI in healthcare. An evaluation of AI's function in biomedical engineering has also taken place. There have been significant advancements in the use of AI in healthcare in recent times [19]. Using AI can help medical facilities become more personalized by providing them with predictive instincts, preventative measures, and the ability to participate in their own care. Drawing on what we know about AI's past performance, we anticipate that it will

continue to develop into a formidable tool for healthcare in the years to come.

Due of recent developments in the field, numerous studies have been conducted to investigate FL based AI-related topics, such as healthcare. For instance, the concepts and protocols underlying FL, as well as the technical challenges associated with FL design and implementation, are presented in the works cited in [9]. [20] discusses some approaches to evaluating dangerous dangers in FL networks and the privacy and security issues in FL systems. Concerns like security, resource allocation, and communication costs are some of the topics covered in the authors' investigation of FL-based AI implementation in [21]. Researchers examine the intersection of FL-AI and the Internet of Things (IoT) in [22], reviewing the technical hurdles in FL schemes (such as sparsification, security, and extensibility) and offering a brief overview of FL-based AI technologies in the IoT [23]. In addition, the authors paid little attention to FL's usage in healthcare in their assessment of FL's applications in industrial IoT ([24]), which focused on FL's characteristics and fundamentals. The requirements and technical hurdles of implementing FL-based AI strategies in the near future of digital health are the subject of another study [25].

2.1 Challenges of Federated Learning

Despite FL's promise of allowing numerous devices to work together on ML model training without exchanging raw data, there are a number of issues that must be resolved [26]. Figure 10 shows a structure of problems related to FL. Here are some of the major obstacles:

Heterogeneity of Data and Devices:

There are many different types of data and devices in the healthcare industry, which makes it difficult to deploy FL efficiently.

• **Data Heterogeneity:** Different types of healthcare data, including text, pictures, and time series, have different properties and necessitate different processing approaches for training models. Device specifications, sensor accuracy, and patient demographics all have a role in the variation in data quality among devices. This is a difficulty. Consequently, FL can't succeed without first pre-processing and standardizing the data.

• **Device Heterogeneity:** There is a wide range in the power consumption, network connectivity, software requirements, and hardware needed by healthcare equipment. The ability to engage in FL may be out of reach for certain devices because to limited resources, such as processing power or memory. More work on data interoperability and communication is also needed because different devices use different operating systems or programming languages. In order for healthcare to overcome disparities in data and equipment, numerous approaches have been developed to tackle this variability in FL.

• **Federated Transfer Learning:** To expedite model training on diverse devices, this approach makes use of pre-trained models on relevant data domains. Adaptive learning algorithms can use the computing power of the device to change the model parameters. It is feasible to reduce data transfer and device computing burden by using efficient communication protocols.

Data privacy and security:

Enhanced privacy and reduced communication costs are just two of the many advantages of this approach, but it poses serious challenges to data protection [27]. Some of the most serious problems that FL has with data privacy are as follows:

• **Leakage of data:** Devices in FL disseminate model updates, however these revisions may still contain sensitive local data. Threat actors may be able to eavesdrop on these changes and use them to learn sensitive information about the local data. Data leaking must be prevented by utilizing encryption and other privacy-protecting technologies.

• **Model inversion attacks:** This issue with privacy could potentially arise in Florida. In order to re-create the original training data used by the local devices, these attacks take advantage of the model updates. To prevent these attacks, it is crucial to implement privacy-preserving methods that secure the local data.

• **Attacks using membership inference:** In FL, attackers with access to certain devices might potentially determine which device was utilized for model training. This data could potentially expose sensitive information about the device's owner or the local data. To thwart membership inference attacks, acy-preserving techniques such as differential privacy can be used.

• **Attacks on the central server:** When using FL, the local devices send model updates to a central

server. Hacked primary server means attacker can access all updates and potentially derive critical information about local data. Consequently, strong security measures must be implemented to protect the central server.

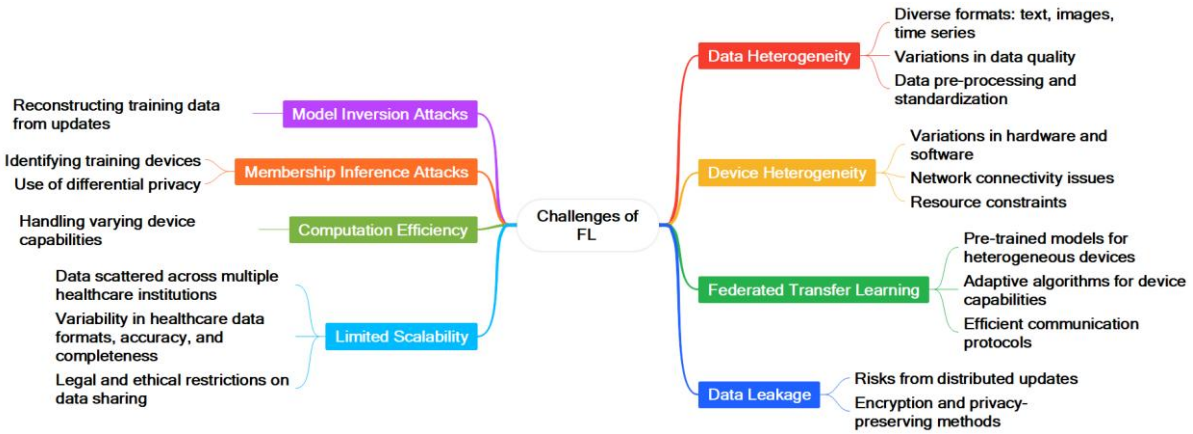

Figure 3: Difficulties with FM in healthcare.

As a whole, FL has a lot of trouble with data privacy protection. Tackling these difficulties calls for a combination of privacy-focused approaches, robust security measures, and meticulous FL system development and execution. In addition, the difficulties of FL in several areas of healthcare are illustrated in Figure 3

2.2 Communication and computation efficiency:

Since FL relies on the secure and timely transmission of data from participating devices to a central server for model training, the efficacy of communication is an important concern [28]. To ensure the models are updated promptly and to protect the privacy of the user's data, the data must be sent with minimal delay. But FL also needs assistance in making its computers more efficient. This means that the model's accuracy could be all over the map, depending on the hardware components used. Plus, training the models with the device's limited resources could lead to battery overconsumption. FL approaches are regularly upgraded to tackle these problems. One possible solution to the issue of communication and computation efficiency is to use model compression techniques to reduce the model's size. This could lead to faster communication. Compute efficiency also with the help of data segmentation, selective participation, and model parallelism. To sum up, improving FL's overall efficacy requires fixing its serious communication and computation efficiency problems. Efforts are ongoing to enhance FL's communication and compute efficiency so that it can continue to be a viable option for ML.

2.3 Handling Non-IID (Independent and Identically Distributed) data:

One of the biggest problems with FL is that it doesn't handle data in an Independent and Identically Distributed (NID) way [29]. The training data in ML is typically thought to be IID, or independent and uniformly distributed. But FL uses a plethora of sources, some of which should be more dispersed or independent, to compile its data. Several issues arise in FL due to the data's non-IID nature. For example, it could be challenging to train a generic model that performs well across all clients due to the fact that data distribution can change substantially between them. There is a risk that training with non-IID data will introduce bias, which could have detrimental effects on performance.

To get around these problems, others have proposed several solutions, such as client weighing, data augmentation, and transfer learning. The process of client weighting entails giving each customer a unique value according to the distribution of their data. This method enhances the model's overall performance by directing training efforts towards clients with more representative data. To make the data more representative, data augmentation involves adding noise or making small changes to the existing data, as well as creating new data samples. Several studies have sought to develop effective FL algorithms for data that does not contain IID, such as FedProx, SCAFFOLD, and FedNova [30]. To solve the problems of non-IID data, one transfer learning strategy is to use a pre-trained model as a starting point for training on the non-IID data.

3. METHODOLOGY

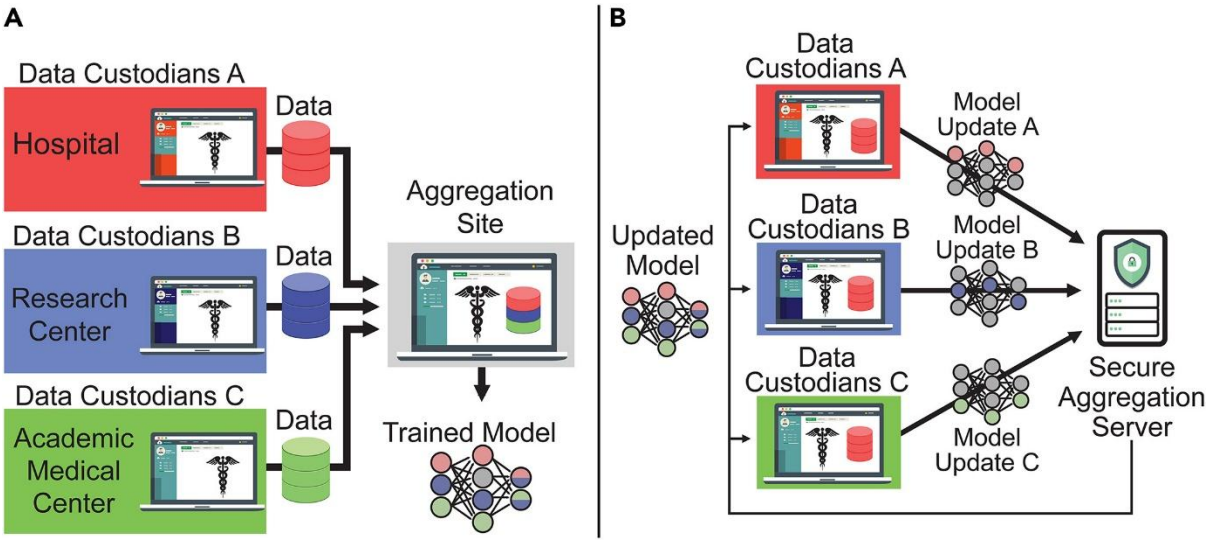

Figure 4. Exemplification of various methods for collaborative learning

(A) In a data-sharing paradigm, all three data custodians send their data to a single location for training. In a federated learning setup, however, each data custodian trains its model independently and only sends its updated model to a secure central server.

There is a lot of hope that AI techniques can improve healthcare workflows. But to train generalizable and stable AI models for clinical applications, you need big and diverse datasets. Collaborative efforts involving multiple institutions, sometimes referred to as "data pooling" (Figure 4A), can help gather enough information. There are a number of reasons why this kind of centralized data collecting isn't always feasible, including worries about patients' privacy, the high expense of data storage and maintenance, and data-sharing regulations at the institutional or even regional levels. Since model learning is done locally at each institution and only the generated local model parameters are shared, federated learning (FL) starts to solve certain privacy concerns, offering an alternative to the data pooling paradigm for multi-institutional cooperation (Figure 4B).

While FL does make it possible to train an AI model on private data without actually sharing it, there are still unanswered questions about why and how to prevent the disclosure of sensitive information through the model updates shared during the FL workflow. More security and privacy features added to FL should allow for a more trustworthy federation, according to those who are hoping for something like this. Institutional information security, compute hardware needs, data preparation coordination and overhead, and trust are just a few of the many obstacles that can discourage institutions from taking part in FL training. More diverse collections of healthcare institutions are likely to be eager to join in FL initiatives if more secure and private FL frameworks are used to increase trust in the system. Better model generalizability may be a consequence of the increased data diversity that can emerge from such partnerships. In industries like healthcare, where data exchange regulations are quite strict, secure and private FL has the potential to significantly improve partnerships.

3.1 Decentralized data and federated machine learning

A lot of people started paying attention to the idea of federated machine learning about 2015. It is a type of distributed system that uses the principle of remote execution, which is sending training iterations and their results (such as updated neural network weights) to a central repository to update the main algorithm. The data is stored on individual sites or devices called nodes. The key advantage is that data can be trained on algorithms without leaving the owner's possession (retention of sovereignty). Full decentralization, for instance, coupled with contribution tracking/audit trails utilizing blockchains, or model sharing across the

nodes and aggregation later on (peer-to-peer/gossip method) are both possible in a federation topology. The ability to conduct training offline and receive results at a later time means that constant access to the internet is unnecessary. As a result, federated learning methodologies are now, in both commercial and healthcare AI contexts, among the most popular next-generation privacy preservation techniques.

Unless paired with the other approaches outlined below, federated learning cannot provide security and privacy, despite its adaptability and success in addressing data ownership and governance concerns. If the data is not encrypted, malicious actors can access the nodes directly and steal sensitive information or disrupt the network. For big data sets or machine learning models, this communication need could be a pain. Verifying the accuracy and reliability of the findings requires data curation, which is made more difficult by the dispersed nature of the data. The best way to update the state of the central model (distributed optimization, federated averaging) needs to be determined via technical study. It is unacceptable from an intellectual property, patent restriction, or asset protection standpoint if data leaks or algorithms are tampered with, rebuilt, or stolen (parameter inference) due to insecurely aggregated updates or unencrypted local algorithms. Neural networks also function as a memory mechanism, as they retain compressed versions of the training data in their weights, which can lead to accidental remembering. Parts of the training data can be reconstructed using the algorithm weights on a decentralized node. It has been demonstrated that images may be recreated with remarkable accuracy and detail, enabling display of the original training data; however, such model inversion or reconstruction assaults might lead to disastrous data leaking. Thus, federated learning provides an infrastructure-level solution to security and privacy; but, more steps are necessary to broaden the scope of its privacy-preserving capabilities, as will be discussed below.

3.2 Real-time monitoring

Users are able to keep tabs on the status and performance of active federated scenarios thanks to Fedstellar's real-time monitoring capabilities. Users are provided with real-time updates on various metrics created by each device in the network architecture using this function. This real-time intelligence allows users to make informed decisions, intervene when necessary, and dynamically measure the experiment's effectiveness. This capability's specialized usage of TensorBoard, a package for visualizing ML experiments, is a key component. That is, the suite is designed to process metrics updated in real-time from multiple devices at once, guaranteeing accurate and quick data representation. The user experience in large-scale federations is greatly improved as metrics loading time is substantially reduced. Better use of network resources and quicker visualization rendering are additional benefits of incorporating a new compression method for TensorBoard events at the controller level. To further guarantee interoperability with other ML/DL libraries, Fedstellar includes an extendable Logger that acts as an adaptor. To make sure everything works together, this Logger converts the metrics it generates into a format that TensorBoard can understand.

The platform also keeps the logging library and the metrics definitions separate. The adaptor may be easily extended to support other popular logging libraries like Wandb, MLFlow, or Neptune, thanks to this design decision. At the same time, customers can still reliably transfer their data to widely-supported formats like CSV or JSON because to the platform's powerful data export capabilities. Users are able to gain a deeper knowledge of how their scenarios performed thanks to this functionality, which allows for smooth data integration with different data analysis and visualization tools.

3.3 Federated Learning for Healthcare Applications

Healthcare Monitoring

FL's ability to facilitate communication between academics and healthcare providers bodes well for the future of healthcare monitoring. The construction of accurate ML models to estimate patient health outcomes is made possible by FL, which pools data from multiple sources such as medical equipment, patient records, and wearable technology. Using information gathered from EHRs, medical devices, and patient-generated data, these models may forecast the likelihood of illness, the likelihood of readmission, and the effectiveness of medications. By keeping tabs on a patient's heart rate, blood pressure, and sleep patterns from a distance, wearable tech like fitness trackers can notify doctors of any irregularities. The proposed frameworks utilize FL to retrain ML models locally with user-generated data while maintaining privacy.

One example is edge-assisted data analytics. To lessen the likelihood of data breaches and illegal access, FL encrypts patient data before storing it locally and transmitting it to a central server. When it comes to healthcare monitoring, FL has the ability to completely transform things by making forecasts more accurate, delivering more targeted care, and protecting patients' privacy.

Medical Imaging

One application of FL in healthcare is medical imaging, where ML techniques are used to decentralize the processing of medical images. Medical imaging plays an essential role in patient diagnosis and treatment, making this technique critical for healthcare. Imaging centers, hospitals, and clinics are common places to find medical imaging data, and they all have their own distinct datasets. With FL, these organizations can work together to train global models, which, as time goes on and more data becomes available, makes illness detection and treatment more effective. By preserving data securely and privately while utilizing collective knowledge from several organizations to improve model development, FL solves privacy concerns that come with centralized data systems. Federated Averaging (FedAvg) and other FL algorithms allow for real-time collaboration across enterprises, which speeds up the creation of models and the detection of diseases. FL improves models' robustness and diagnostic accuracy by resolving data imbalance issues prevalent in medical imaging through data pooling from multiple sources. In the realm of medical imaging, FL holds great potential for better patient outcomes and lower healthcare expenditures.

Electronic Health Record

Clinical decision-making within EHR systems could be greatly improved by FL. Google first suggested FL for board question recommendation; it entails training a global model with data from many sources, such as wearable gadgets, hospital systems, and personal health information. Every participant's device updates the global model by first training it locally and then aggregating its parameters. FL eliminates the need to transfer data in order to solve the problem of data silos in electronic health record systems, enabling more diversified and comprehensive datasets to provide insights and forecasts.

Take FL and blockchain technology head-on to tackle the problems associated with data management and security, which are major concerns with electronic health records (EHRs). Motivating FL involvement, reliable model aggregation, and managing the massive amount of EHR data are all problems they take on. Their suggested approach improves interoperability by combining blockchain technology with cloud services, but it does so at the expense of EHRs' immutability. Updates to electronic health records (EHRs) may take longer than expected if blockchain integration causes extra validation stages.

4. RESULTS AND DISCUSSION

Table 1. Assets related to FL security and privacy, particularly CIA properties that we aim to tackle in our study

Asset	Confidentiality	Integrity	Availability
Data Training	✓	✓	✗
Metrics of Quantitative	✓	✗	✗
Model parameters	✓	✓	✗
Hardware	✗	✗	✗
Source code	✓	✓	✗
Additional files or information	✓	✓	✗

The assets and their qualities that will be addressed in this study are summarized in Table 1. Each of the CIA's features will be defined and discussed in further detail in the sections that follow. From a high level, we expect hardware protection to already be in place. Participants are expected to report correct validation metrics with minimal privacy consequences. We do not address issues of unavailable FL system resources because we do not

see minimal privacy impact to participants dropping out or losing network connections.

Confidentiality

In this context, "confidentiality" means how well-kept the asset is. Take the case of collaborator A who uses transport layer security (TLS) to transmit their model update to the aggregator. TLS provides A with certain guarantees regarding the update's confidentiality during transmission. The extent to which the update remains confidential after receiving and decryption in TLS by the aggregator depends on the aggregator's code logic (it could just broadcast it to others, for instance) and the level of protection the aggregator processes have against other processes and users on the aggregator infrastructure.

Integrity

In this context, "integrity" refers to how well the asset meets expectations. Collaborant A may, for instance, wish to verify that code executed on Collaborant B's computing infrastructure is secure. To the degree that A is certain of the integrity of B's infrastructure, A may in rare instances trust B with its operations.

Availability

When we talk about an asset's "availability," we mean how accessible it is. Consider the following scenarios: the aggregator may not have access to local model updates due to a collaborator's downed network infrastructure, or the entire federation could experience difficulties due to a loss of network connection at the aggregator level. Table 2 summarizes all of the privacy threats examined in this review, along with the types of threat mitigation techniques. Because each method provides a unique set of safeguards, the best approach to take in any given situation will vary.

Table 2. Methods for improving privacy and the qualities that should be considered for their implementation

Technique	SMPC	HE	CC	DP	PAMO
Disclosure of data used	Yes	no	no	yes	yes
Data usage integrity	No	no	no	medium	no
Discoveries exposed to data mining	No	yes	yes	no	no
A reliable execution	Based on protocol	no	yes	no	no
Performance impact (depending on the implementation)	high	high	yes	yes	medium
Equal mathematical weight to the initial findings	yes	yes	medium	no	no
Threats mitigated	Threats of a system	Threats of a system	security risks, data mining, poisoning	extraction of information	extraction of information

Each row is the property and the head of each column is the name of a privacy-enhancing technique. In controlled use, SMPC, HE, and CC safeguard assets, but they do not prevent an adversary from discovering sensitive information in the final results ("results unprotected from information extraction") or from discovering sensitive information in the intermediate results ("exposure of data in use"). While free-use mitigation strategies like DP and PAMO do limit the ability to infer information about the original inputs from the final result of the computation, they do nothing to address the confidentiality of inputs or intermediate results on their own. While other types of mitigations typically do not guarantee the accuracy of the calculations ("execution integrity"), CC-category mitigations may.

CONCLUSION

Through maintaining the emphasis on FL in a healthcare context, we offer a taxonomy and a more thorough comprehension of present privacy issues along with their corresponding mitigation strategies. While providing the reader with basic concepts that may be utilized in this field, we have also offered extensive explanations of potential privacy

infractions and measures to minimize them, including a relevant categorization for both. Our investigation into the validity of these methods in relation to FL for healthcare has started since there is growing proof that FL could usher in a new era in which different healthcare organizations can work together to build AI models without disclosing any of their local data. Also included in this research is the use of Federated Learning (FL) in healthcare, specifically how it might improve the safety and confidentiality of patient information. Based on our research, FL has the potential to greatly reduce vulnerabilities like data leakage and model inversion attacks by utilizing procedures like safe aggregation and differential privacy.

REFERENCES

[1] Muhammad, G., Alshehri, F., Karray, F., El Saddik, A., Alsulaiman, M., Falk, T.H.: A comprehensive survey on multimodal medical signals fusion for smart healthcare systems. Information Fusion **76**, 355–375 (2021)

[2] Nguyen, D.C., Cheng, P., Ding, M., Lopez-Perez, D., Pathirana, P.N., Li, J., Seneviratne, A., Li, Y., Poor, H.V.: Enabling ai in future wireless networks: a data life cycle perspective. IEEE Commun Sur Tutorials **23**(1), 553–595 (2020)

[3] Shickel, B., Tighe, P.J., Bihorac, A., Rashidi, P.: Deep ehr: a survey of recent advances in deep learning techniques for electronic health record (ehr) analysis. IEEE J. Biomed. Health Informat. **22**(5), 1589–1604 (2017)

[4] Li, D., Luo, Z., Cao, B.: Blockchain-based federated learning methodologies in smart environments. Cluster Computing pp. 1–15 (2021)

[5] Rahman, A., Islam, M.J., Saikat Islam Khan, M., Kabir, S., Pritom, A.I., Razaul Karim, M.: Block-sdotcloud: Enhancing security of cloud storage through blockchain-based sdn in iot network. In: 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), pp. 1–6 (2020). https://doi.org/10.1109/STI50764.2020.9350419

[6] Islam, M.J., Rahman, A., Kabir, S., Khatun, A., Pritom, A., Chowdhury, M.: Sdot-nfv: A distributed sdn based security system with iot for smart city environments. GUB Journal of Science and Engineering **7**, 27–35 (2021) https://doi.org/10.3329/gubjse.v7i0.54015. https://www.banglajol.info/index.php/GUBJSE/article/view/54015

[7] Hossen, R., Whaiduzzaman, M., Uddin, M.N., Islam, M., Faruqui, N., Barros, A., Sookhak, M., Mahi, M., Nayeen, J., et al.: Bdps: An efficient spark-based big data processing scheme for cloud fog-iot orchestration. Information **12**(12), 517 (2021)

[8] Cheng, V.S., Hung, P.C.: Health insurance portability and accountability act (hippa) compliant access control model for web services. Int. J. Healthcare Informat. Sys. Informatics (IJHISI) **1**(1), 22–39 (2006)

[9] Nguyen, D.C., Pham, Q.V., Pathirana, P.N., Ding, M., Seneviratne, A., Lin, Z., Dobre, O.A., Hwang, W.J.: Federated learning for smart healthcare: A survey. arXiv preprint arXiv:2111.08834 (2021)

[10] Sheller, M.J., Reina, G.A., Edwards, B., Martin, J., Bakas, S.: Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation. In: International MICCAI Brainlesion Workshop, pp. 92–104. Springer (2018)

[11] Warnat-Herresthal, S., Schultze, H., Shastry, K.L., Manamohan, S., Mukherjee, S., Garg, V., Sarveswara, R., Händler, K., Pickkers, P., Aziz, N.A., et al.: Swarm learning for decentralized and confidential clinical machine learning. Nature **594**(7862), 265–270 (2021)

[12] Sheller, M.J., Edwards, B., Reina, G.A., Martin, J., Pati, S., Kotrotsou, A., Milchenko, M., Xu, W., Marcus, D., Colen, R.R., et al.: Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data. Scientific Reports **10**(1), 1–12 (2020)

[13] Kaissis, G., Ziller, A., Passerat-Palmbach, J., Ryffel, T., Usynin, D., Trask, A., Lima, I., Mancuso, J., Jungmann, F., Steinborn, M.M., et al.: End-to-end privacy preserving deep learning on multi-institutional medical imaging. Nat. Mach. Intell. **3**(6), 473–484 (2021)

[14] Kaissis, G.A., Makowski, M.R., Rückert, D., Braren, R.F.: Secure, privacy-preserving and federated machine learning in medical imaging. Nat. Mach. Intell. **2**(6), 305–311 (2020)

[15] Rahman, A., Islam, M.J., Sunny, F.A., Nasir, M.K.: Distblocksdn: A distributed secure blockchain based sdn-iot architecture with nfv implementation for smart cities. In: 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET), pp. 1–6 (2019). https://doi.org/10.1109/ICIET48527.2019.9290627

[16] Yu, K.H., Beam, A.L., Kohane, I.S.: Artificial intelligence in healthcare. Nat. Biomed. Eng. **2**(10), 719–731 (2018)

[17] Peng, Y., Zhang, Y., Wang, L.: Guest editorial: Artificial intelligence in biomedical engineering and informatics: An introduction and review. Artificial Intell. Med. **48**(2–3), 71–73 (2010)

[18] Gupta, D., Kayode, O., Bhatt, S., Gupta, M., Tosun, A.S.: Hierarchical federated learning based anomaly detection using digital twins for smart healthcare. arXiv preprint arXiv:2111.12241 (2021)

[19] Arikumar, K., Prathiba, S.B., Alazab, M., Gadekallu, T.R., Pandya, S., Khan, J.M., Moorthy, R.S.: Fl-pmi: Federated learning-based person movement identification through wearable devices in smart healthcare systems. Sensors **22**(4), 1377 (2022)

[20] Mothukuri, V., Parizi, R.M., Pouriyeh, S., Huang, Y., Dehghantanha, A., Srivastava, G.: A survey on security and privacy of federated learning. Future Generat. Comput. Sys. **115**, 619–640 (2021)

[21] Lim, W.Y.B., Luong, N.C., Hoang, D.T., Jiao, Y., Liang, Y.C., Yang, Q., Niyato, D., Miao, C.: Federated learning in mobile edge networks: A comprehensive survey. IEEE Commun. Surv. Tutorials **22**(3), 2031–2063 (2020)

[22] Khan, L.U., Saad, W., Han, Z., Hossain, E., Hong, C.S.: Federated learning for internet of things: Recent advances, taxonomy, and open challenges. IEEE Communications Surveys & Tutorials (2021)

[23] Islam, M.J., Rahman, A., Kabir, S., Karim, M.R., Acharjee, U.K., Nasir, M.K., Band, S.S., Sookhak, M., Wu, S.: Blockchain-sdn based energy-aware and distributed secure architecture for iots in smart cities. IEEE Internet of Things J. (2021). https://doi.org/10.1109/JIOT.2021.3100797

[24] Pham, Q.V., Dev, K., Maddikunta, P.K.R., Gadekallu, T.R., Huynh-The, T., et al.: Fusion of federated learning and industrial internet of things: a survey. arXiv preprint arXiv:2101.00798 (2021)

[25] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H.R., Albarqouni, S., Bakas, S., Galtier, M.N., Landman, B.A., Maier-Hein, K., et al.: The future of digital health with federated learning. NPJ Digital Medicine **3**(1), 1–7 (2020)

[26] Muhammad Mateen Yaqoob, Muhammad Nazir, Muhammad Amir Khan, Sajida Qureshi, and Amal Al-Rasheed.Hybrid classifier-based federated learning in health service providers for cardiovascular disease prediction.*Applied Sciences*, 13(3):1911, 2023.

[27] Akhil Vaid, Suraj K Jaladanki, Jie Xu, Shelly Teng, Arvind Kumar, Samuel Lee, Sulaiman Somani, Ishan Paranjpe, Jessica K De Freitas, Tingyi Wanyan, et al.Federated learning of electronic health records to improve mortality prediction in hospitalized patients with covid-19: machine learning approach.*JMIR medical informatics*, 9(1):e24207, 2021.

[28] Gokberk Elmas, Salman UH Dar, Yilmaz Korkmaz, Emir Ceyani, Burak Susam, Muzaffer Ozbey, Salman Avestimehr, and Tolga Çukur.Federated learning of generative image priors for mri reconstruction.*IEEE Transactions on Medical Imaging*, 2022.

[29] Rajesh Kumar, Abdullah Aman Khan, Jay Kumar, Noorbakhsh Amiri Golilarz, Simin Zhang, Yang Ting, Chengyu Zheng, Wenyong Wang, et al.Blockchain-federated-learning and deep learning models for covid-19 detection using ct imaging.*IEEE Sensors Journal*, 21(14):16301–16314, 2021.

[30] Xiaoxiao Li, Yufeng Gu, Nicha Dvornek, Lawrence H Staib, Pamela Ventola, and James S Duncan.Multi-site fmri analysis using privacy-preserving federated learning and domain adaptation: Abide results.*Medical Image Analysis*, 65:101765, 2020.